SMALL BUSINESS ADMINISTRATION
STANDARD OPERATION PROCEDURE

AUTOMATED INFORMATION SYSTEMS SECURITY PROGRAM 90 47 1

INTRODUCTION

1. **Purpose:** To establish guidelines and procedures for Automated Information Systems Security.

2. **Personnel Concerned:** All SBA employees and contractors who use automated information systems.

3. **Originator:** Office of the Chief Information Officer.

Printed copies of the manual might not be current, refer to the electronic version maintained by the OCIO.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1. What is the Purpose of the Small Business Administration's (SBA) Automated Information Systems (AIS) Security Program?

The purpose of the Small Business Administration's (SBA) Automated Information Systems (AIS) Security Program is to assure adequate protection of SBA automated information processed and maintained by the Agency's computer systems.

An AIS Security Program must be in effect at SBA to assure that computerized data and other valuable Agency resources controlled by computers are safeguarded from inadvertent or deliberate disclosure, modification, destruction, or misuse. A full-time Agency Computer Security Program Manager (ACSPM), located in the Office of the Chief Information Officer (OCIO), will manage this program.

In accordance with the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources", Appendix III, " Security of Federal Automated Information Systems", the SBA AIS Security Program must include:

a. A personnel security program must be in effect for all personnel, both Federal and contractor, who are involved with the operation, maintenance, or use of AIS installations and sensitive, automated applications. This program must be in accordance with guidance from the Office of Personnel Management.

b. A security awareness and training program must be implemented to assure that all individuals involved with the operation, maintenance, or use of AIS installations or sensitive, automated applications are aware of AIS security policies and procedures.

c. Sensitivity determinations must be made of all data contained in AIS installations or automated applications within SBA.

d. A risk assessment program must be in effect for AIS installations to evaluate vulnerabilities in these installations, and to ensure that cost-effective controls are identified and implemented.

e. A security evaluation program must be in effect to identify vulnerabilities existing in sensitive automated applications. Appropriate cost-effective safeguards must be identified and implemented during the annual internal control process carried out by the respective program office element per the Agency Internal Control requirements of OMB Circular A-123, "Management Accountability and Control".

f. A management control process must be in effect to assure that appropriate administrative, physical, personnel, and technical AIS security requirements are specified in bid offerings, proposals, and contracts for AIS equipment and services.

g. An Agency continuity of operations program must be in effect to ensure that critical Agency applications and systems maintained at AIS installations are available and operable in the event computer processing is not available, i.e., SBA AIS installations are incapacitated.

h. Security responsibilities must be defined and assigned in writing to specific individuals.

i. Security plans must be prepared and tested for each major application and general support system.

j. System usage must be authorized in writing and be reviewed and reauthorized at least every three years.

k. All users must receive specialized system and security training including security responsibilities before they are allowed access to a system.

l. Material weakness and deficiencies in systems must be identified in the annual Federal Manager's Financial Integrity Act (FMFIA) report.

m. A summary of systems security plans and major applications plans must be included in the strategic plan required by the Paperwork Reduction Act of 1995, 44 U.S.C. Section 3506.

2. What Rule Governs the AIS Security Program?

The AIS Security Program is mandated by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems."

3. What is SBA's General AIS Security Policies?

SBA employees and contractors are permitted "limited personal" use of Government office equipment including information technology (IT) if the use does not interfere with official business and involves minimal additional expense to the Government as specified in the March 23, 1999 Federal CIO Council Review Approval of Limited Personal Use Policy of Government Office Equipment. Limited personal use should take place during the employee's personal time, not during official duty time. This privilege to use Government office equipment for non-government purposes may be revoked or limited at any time by appropriate SBA officials.

Government office equipment including IT includes, but not limited to: personal computers and related peripheral equipment and software, library resources, telephones, facsimile machines, photocopiers, office supplies, E-mail, and Internet connectivity and access to Internet services.

Employees and contractors are expected to conduct themselves professionally in the workplace and to refrain from using Government resources for activities that are inappropriate or offensive to co-workers or the public, such as the use of sexually explicit materials or remarks that ridicule others on the basis of race, creed, religion, color, sex, handicap, national origin, or sexual orientation.

While occasional use of Government office equipment in moderation is acceptable; uses not conforming to this policy are strictly prohibited. Official Government business always takes precedence over the limited personal use.

This limited personal use must not result in loss of employee and contractor productivity or interference with official duties and incurs only minimal additional expense to the Government in areas such as:

a. Communications infrastructure costs: e.g., telephone charges, telecommunications traffic, etc.

b. Use of consumables in limited amounts: e.g., paper, ink, toner, etc.

c. General wear and tear on equipment.

d. Minimal data storage on storage devices.

e. Minimal transmission impacts with moderate message sizes such as E-mails with small attachments.

Personal time means non-work hours such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, weekends, or holidays (if their duty station is normally available).

4. What are Inappropriate Limited Personal Uses of Government Office Equipment?

Employees and contractors are expected to conduct themselves professionally in the workplace and to refrain from using Government office equipment and IT for activities that are inappropriate. Misuse or inappropriate personal use of Government office equipment includes, but not limited to:

a. Any personal use that could cause congestion, delay, or disruption of service to any Government system or equipment. For example: greeting cards, video, sound or other large file attachments can degrade the performance of the entire network. “Push” technology on the Internet and other continuous data streams would also degrade the performance of the entire network and be an inappropriate use.

b. Using the Government systems as a staging ground or platform to gain unauthorized access to other systems.

c. Creating, copying, transmitting, or retransmitting chain letters or other authorized mass mailings regardless of the subject matter.

d. Activities that are illegal, inappropriate, or offensive to fellow employees or the public. These activities include, but not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

e. Creating, downloading, viewing, storing, copying, transmitting, or retransmitting sexually explicit or sexually oriented materials or materials related to gambling, weapons, terrorist activities, and activities otherwise prohibited.

f. Use of commercial purposes or in support of “for-profit” activities or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sale of goods, or services).

g. Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity, not authorized by government ethics rules.

h. Use for posting Agency information to external newsgroup, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one’s official capacity as a Federal Government employee, unless appropriate Agency approval has been obtained or uses at odds with the Agencies mission of positions.

i. Any use that could generate more than minimal additional expense to the Government.

j. Unauthorized acquisition, use, reproduction, transmission, and distribution of computer software or other material protected by national and international copyright laws, trademarks, or other intellectual property rights.

k. Playing on-line games.

l. Representing oneself as someone else.

m. Soliciting Government employees or providing information about or lists of Government employees to others outside the Government without authorization.

n. When it interferes with the employee’s or contractors’ job, the jobs of other individuals, operation of SBA, or the Internet gateways.

o. Any type of personal solicitation.

p. Modifying Government office equipment for non-government purposes, including loading personal software or making configuration changes.

q. Government resources and official time shall not be used to earn outside income or private gain.
r. Employees and contractors shall not record overtime, compensatory time, or credit hours earned during any period of time when using Government office equipment for limited personal use.

CHAPTER 2

RESPONSIBILITIES

1. What are the Responsibilities of the SBA Administrator?

The SBA Administrator is responsible for establishing a management control process to ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications. The Administrator has delegated this responsibility to the Chief Information Officer (CIO).

2. What are the Responsibilities of the CIO?

The CIO has been delegated the overall responsibility for the development and implementation of the Agency computer security program. The CIO is responsible for:

a. Designating a management official, the ACSPM, who will have overall responsibility for the development and implementation of the Agency computer security program.

b. Establishing policies, standards, and procedures to assure that specific administrative, physical and technical security controls are in place and working properly for SBA's automated environment.

3. What are the Responsibilities of the ACSPM?

The responsibilities of the ACSPM are to:

a. Develop and implement an Agency AIS Security Program consistent with Government-wide policies, procedures, and standards, which includes applications security, personnel security, and security for computer installations.

b. Develop and disseminate computer security policy and standards for the SBA AIS Security Program.

c. Ensure that an appropriate level of security is maintained at all SBA computer installations.

d. Establish a program for periodic security and internal control reviews at each computer installation.

e. Monitor the establishment and maintenance of a comprehensive continuity of operations plan for each computer installation.

f. Establish a security awareness program to ensure that Agency and contractor personnel are aware of their security responsibilities and know how to fulfill them.

g. Establish an incident response and reporting capability.

h. Provide guidance and recommendations with respect to Agency data sensitivity and determinations.

i. Establish a process to ensure that implementation of OMB Circulars A-130 and A-123 is coordinated to maximize the effectiveness of computer security and internal control procedures employed.

j. Conduct vulnerability assessments on Agency automated data processing (ADP) resources and assist SBA managers in the determination of associated threats to ADP resources.

k. Keep current Agency SOPs and other directives on AIS security matters.

l. Refer all suspected criminal violations, including theft of computer hardware and software, to the OIG, Investigations Division.

m. Coordinate with the Office of the Inspector General (OIG), Investigations Division, in the investigation of AIS security breaches and recommend emergency procedures deemed necessary.

n. Assist the designated Agency official responsible for meeting the requirements of the Privacy Act of 1974 (P.L. 93-579, Title 5 U.S.C. 552a).

4. What are the Responsibilities of the Computer Emergency Response Team (CERT)?

The Computer Emergency Response Team (CERT) was established to investigate computer security-related incidents under the supervision of the ACSPM. The CERT has review and disposition authority for incidents assigned to it. The CERT includes personnel from the Office of the Chief Information Officer. Headquarters program personnel, district Information Resource Managers (IRMs) and ESC Security Officer will be included on an ad hoc basis, when appropriate. The CERT will report its findings to the Chief Information Officer for transmittal to the affected organization and the Administrator. Security incidents should be reported to the ACSPM at (202) 205-6708.

5. What are the Responsibilities of the Management Board?

Under revised OMB Circular A-130, Appendix III, functional program managers are responsible for ensuring the security and integrity of their automated information processing systems. OCIO will coordinate its security reviews with the appropriate Management Board members to ensure that adequate procedures and controls are in place to ensure the security and integrity of their systems.

6. What are the Responsibilities of the District Directors, Office Managers, and Disaster Area Office Directors?

District Directors, Office Managers, and Disaster Area Office Directors are responsible for:

a. Implementing procedures to ensure that administrative, physical, and technical security controls are in place for local computing activities.

b. Maintaining appropriate security controls in sensitive, automated applications maintained on local computing equipment.

7. What are the Responsibilities of District AIS Security Officers (DSO)?

District AIS Security Officers (DSO) are responsible for:

a. Using the special password generating transaction to generate passwords for users of the mainframe data communications network who must have access to sensitive/critical transactions.

b. Implementing procedures to ensure that administrative, physical, and technical security controls are in place for local computing activities.

c. Maintaining appropriate security controls in sensitive automated applications maintained on local computing equipment.

d. Implementing an AIS contingency plan which addresses the timely recovery of data processing operations at the district office.

8. What are the Responsibilities of the Unisys Corporation Eagan Service Center AIS Security Officer (ESC Security Officer)?

The responsibilities of the Unisys Corporation ESC Security Officer are to:

a. Ensure that an appropriate level of security is maintained for the Eagan Service Center to protect the computer center against breeches of security.

b. Assist the ACSPM in the investigation of AIS security breaches that affect processing at the Eagan Service Center.

c. At the direction of the ACSPM implement Agency AIS policies, procedures, and standards which affect the Agency computer installations in the Eagan Service Center.

d. Represent Unisys Corporation as the focal point for periodic information security audits and internal control reviews conducted at the Eagan computer facility.

e. Recommend security enhancements and improvements where appropriate.

9. What are my Responsibilities if I am a User of Automated Information Systems?

a. All SBA employees and contractors have AIS security responsibilities. You are responsible and accountable for actions taken while using an automated application or accessing a computer installation. Actions attributed to the user's identification and password combination must be examined to identify the originator of any abusive actions occurring within the automated application or computer installation.

b. You are responsible for being familiar with and complying with all Agency standards, policies, and procedures established pursuant to the AIS Security Program, both as identified in this chapter and pursuant to instructions issued by the AIS Security Officers.

c. You are responsible for changing your password every 90 days. Your new password must not be an easily guessed combination of letters or characters. Good passwords are passwords that are difficult to guess. The best choices for constructing a password uses the full 95 character keyboard set, (uppercase and lowercase letters; digits, and punctuation characters), yet is easy to remember. While constructing your password avoid names, telephone and license numbers, or other information easily obtained about you. Passwords must not be hard coded into programs, written down, or programmed into PC function keys.

d. You must not leave your workstation unattended while accessing a computer installation or automated application. Workstations should be protected using a password-protected screen that secures the workstation after 10 minutes of inactivity.

e. Report security incidents to your supervisor, security coordinator, or ACSPM.

f. Install on your PC and maintain current the Agency approved virus protection software. Ensure that it runs on your PC at startup. Report PC viruses to your security coordinator.

CHAPTER 3

AIS SECURITY POLICIES

1. What Security Controls are Required for Existing AIS Installations and Computer Facilities contracted by the Agency?

The following minimum controls must be in effect for SBA data processing facilities or data processing facilities contracted by the Agency to house its computer system(s) and networking equipment. Agency management may implement additional security controls when supported by risk assessment analysis:

a. Security management. Responsibility for day-to-day security of the SBA Data Processing facilities must be assigned to a specific individual knowledgeable in data processing technology and computer security methodology.

b. Automated physical security controls must be in place to limit physical access to authorized personnel.

c. Controls must be implemented to safeguard computer media.

d. Operating system software must contain adequate security controls to minimize the likelihood of unauthorized access to or use of system resources.

e. There must be a statement that declares to the user at login time that the system is protected against inappropriate use and violators will be prosecuted to the fullest extent of the law.

f. Password change screens must revalidate the old password and new password. The new password must be typed in a secure field to prevent compromise.

g. User Access controls. Control procedures must include the following:

(1) Passwords must be used to authenticate the account user. User accounts and passwords may not be shared between individuals.

(2) A user's password must be changed immediately if there is a reason to suspect that the password has been compromised. When necessary administrators must be able to assign new passwords after confirming the users identity.

(3) Passwords must be protected by administrative, physical, and technical security controls from unauthorized disclosure or misuse.

(4) Passwords must be at least eight characters in length, must not be easily guessed combinations (e.g., all zeros, dashes, etc.), and must not be the same as the user-id. Note: the ACSPM has granted an exception for the QTERM application. This exception allows user passwords of six (6) characters in length. QTERM users will be revalidated once each calendar year.

(5) Users must be able to change their own passwords and passwords must set to automatically expire every 90 days.

(6) The initial password or a reissued password must be forced to change with the first use. A forgotten password will be replaced not reissued.

(7) Accounts will be suspended as quickly as possible but no greater than three working days from the time the user is no longer authorized access to the computer installation or computer application. Inactive accounts must be suspended after 120 days of inactivity.

(8) Expiration dates must be assigned to temporary accounts.

(9) A history of eight passwords must be maintained before a password can be reused.

h. Information Backup. System software and data must be backed up on a regular basis. Full system backups must be performed at least once weekly. Incremental data backups (backups of data that has changed since the last full backup) must be performed nightly. The backup procedure must include the production of a second set of backup media which is stored offsite in an approved data repository. Additional backups may be taken as necessary.

i. Monitoring user activity. Security log files must be reviewed on a regular basis to detect unauthorized access to sensitive data, misuse of the computer system, or other unauthorized activity.

j. Auxiliary Power. The computer facility must be equipped with auxiliary power generating facilities, which will provide sufficient power to allow graceful system shutdown in the event of a power failure.

k. Remote Access security controls. These security measures must include:

(1) The use of communications servers to permit remote dial-in access to SBA's wide area network.

(2) The use of secure servers for INTERNET access to SBA's wide area network.

l. Personnel Security. The following personnel security controls must be in place for the SBA Data Processing Service:

(1) Sensitive ADP positions must be identified and forwarded to the Office of Human Resources in accordance with instructions furnished by that office.

(2) Contractors filling sensitive ADP positions are required to meet the same personnel security requirements as their Federal employee counterparts.

2. <u>What Security Controls are Required for Mainframe Computers?</u>

a. Security Management. Responsibility for day-to-day security of the data processing facility must be assigned to a specific individual knowledgeable in data processing technology and computer security methodology.

b. Using SIMON, the ACSPM or designated District AIS Security Officer will establish the initial user account and password or reissue a user’s password after proper user verification.

c. User validation must occur at “login” or the initial connection to the computer environment.

d. Users will be granted full access (read/write authority) to their personal data areas and the common shared area. Access to Application areas will be restricted to 'read only'. Access to System areas will be restricted to the ESC system administrator.

e. Accounts will be deleted immediately when a SBA or ESC employee leaves the organization. Other user accounts will be monitored periodically to remove inactive accounts.

f. Accounts must be locked after three (3) invalid access attempts. Where possible the station should be locked to prevent the user from repeating the attempts.

g. Workstations should be logged out after 10 minutes of inactivity.

h. OCIO must approve connections to the private network from any source outside the network before connection attempts are made.

3. What are the Security Controls for Desktop Computers?

a. The following minimum security controls will apply to Desktop Computer usage in SBA:

(1) Responsibility for the protection of the hardware, system software, and sensitive data will be assigned to the program manager with operational responsibility for the organization.

(2) Desktop Computers must be maintained in a secure environment. Desktop Computer equipment located in open areas should be secured to the desk when possible.

(3) Desktop computers should be protected using a password-protected screen that secures the workstation after 10 minutes of inactivity.

(4) Disks containing valuable information must be backed up at least monthly to protect against permanent loss, should the original disk become damaged or stolen.

(5) Agency standard Desktop Computer virus detection and eradication software must be installed on all Agency Desktop Computers. The software must be installed in such a manner as to be loaded each time the system is turned on or reset (rebooted via CTRL-ALT-DEL). Virus detection software updates must be applied as soon as available to maintain the maximum level of protection against viruses.

(6) Files and diskettes received from any source must be scanned for viruses before being used on Agency systems.

(7) Additional controls may be instituted where warranted.

b. Desktop Computer Software Distribution.

The following guidelines must be followed when distributing or receiving Desktop Computer software:

(1) Field Information Technology Specialists (FITS) must coordinate and control the distribution of Desktop Computer software to regional and district offices. Software intended for regional or district office use must be sent directly to the FITS for security analysis and distribution.

(2) District IRMs must scan all software received, regardless of source, prior to releasing or loading it.

(3) Regional and district program personnel receiving software from vendors or Headquarters must submit the software to their FITS or District IRMs for analysis before loading it. District IRMs receiving software from vendors, Headquarters, or district personnel must contact their FITS for clearance prior to releasing or loading it.

(4) In Headquarters, OCIO will be the review point for software developed or provided for general distribution. All such software must be submitted to OCIO for security analysis prior to being released or loaded.

(5) Headquarters program offices must scan all commercial software obtained for internal use prior to loading it.

c. Copyrighted Desktop Computer Software.

The following Desktop Computer software copyright policy is established:

(1) An employee of the SBA must not copy, except as provided below, any software that is protected by a copyright unless authorized by the software license agreement which accompanies such software.

(2) In order to protect the Agency's investment in software and to ensure the operational continuity of Agency programs, it is permissible to make a backup copy of copyrighted software.

(3) The removal of Desktop Computer software that has been purchased by the Agency from any Government owned Desktop Computer, office or building for purposes other than official business is prohibited. Installation of software obtained in violation of copyright restrictions on Agency computers is also strictly prohibited.

(4) This policy applies equally to employees of the Agency, contract or grant employees doing business with or acting for the Agency, and any others who may have access to or be required to use commercial software in the performance of their assignments.

(5) Employees violating this policy will be subject to appropriate disciplinary action.

(6) Should the owners, vendors, or authorized custodians of copyrighted software choose to sue the individuals concerned and, if the Agency determines such copying was illegal and unauthorized by SBA, the Agency may choose not to provide any support, legal or otherwise.

4. What are the Security Controls for UNIX-Based Computers?

Computers running the UNIX operating system require special security precautions. Improper setup or misuse of UNIX-based computers can jeopardize the security of the SBA network. Therefore, any individual wishing to acquire UNIX-based computers must receive authorization from the CIO before acquiring the system(s). OCIO will coordinate the installation and configuration of the system(s) to ensure that they pose no security risk. Configuration must include the installation of OCIO user accounts on the systems to aid in problem analysis and in security evaluations. OCIO accounts will not be placed on single-user Desktop Computers.

Because the UNIX operating system can be installed on any type of computer, laptop to mainframe, the following guidelines apply to all systems running the UNIX operating system:

a. The SUPERUSER account (ROOT) must be protected with a password of at least eight characters, two of which must be special characters (!,$,%,*). Root Passwords must be changed at least once every two months. Passwords should be changed more frequently as conditions warrant.

b. All user accounts must be protected by passwords of at least eight characters, two of which must be non-alphabetic (i.e., numeric or special) characters. At a minimum, user passwords must be changed once every 90 days.

c. Users must not create files that are World Writable, that is writable by anyone. This will ensure that files are not deleted, altered, moved, or mismanaged by anyone other than the owner or group associated with the file. Files, at a minimum, should have the write bit for "other" removed from the file permissions.

d. UNIX-based computers requiring remote user login access must have authentication software installed which generates one-time passwords. The current Agency standard software is Lockout DES.

e. UNIX-based computers that do not require remote access must have all remote services/utilities disabled. When possible, users should be isolated from the operating system through the use of user interfaces or menus.

f. Modems must not be connected to UNIX-based systems. Access to external information sources (e.g., INTERNET) must be made through the Wide Area Network. Direct connections are prohibited.

g. System software and data must be backed up on a regular basis. Full system backups must be performed at least once weekly. Incremental data backups (data that has changed since the last full backup) must be performed nightly. The backup procedure must include the production of a second set of backup media, which is stored offsite in an approved data repository. Additional backups may be taken and stored as necessary.

h. A programmable uninterruptable power supply (UPS) capable of supplying power for at least fifteen minutes must be installed on each machine. The UPS must be programmed to gracefully shut down the computer when five minutes of UPS power remain.

Types of UNIX Servers include*:*

a. Client Servers - In addition to the foregoing, the following guidelines apply to client servers:

(1) Users must access client servers through approved client front-end software provided by OCIO. Other access methods are prohibited.

(2) Client server accounts must be established by the ACSPM upon presentation of a request signed by the appropriate program manager. Client server accounts may not be shared. Users must not divulge their passwords to others.

(3) The "/etc/ftpusers" file should be maintained to limit users access to FTP. Any Userids not listed in /etc/ftpusers are allowed to transfer files using FTP. At a minimum, this file should contain the root userid and other accounts generated by the UNIX operating system.

(4) The root crontab should monitored for cron entries that execute scripts that don't exist. In cases like this, any user can simply create the script specified, and thus have "root" execute any command the user desires.

(5) All systems should be closed systems, not allowing access via another host's security. Systems should be monitored for the presence of ".rhost" files and "/etc/hosts.equiv" files. Entries in these files give outside users access to the current system using remote shell commands.

(6) Userids that are deleted from the system should have their files either removed from the system or have their ownership given to another Userid on the system.

(7) Users that successfully use the switch user command "su" will be logged and monitored. The “su” log will report use of the "root" privileged activities.

(8) Client server systems will be operated and maintained by OCIO.

b. World Wide Web Servers - In addition to the foregoing general guidelines, the following guidelines apply to Agency Web servers:

(1) UNIX-level user accounts will not be permitted on Web servers.

(2) Users must access Web servers through standard web browsers.

(3) Web servers are for the dissemination of publicly available Agency information. Sensitive information relating to businesses or individuals doing business with SBA must not be placed on Web servers. Information intended for dissemination via Web servers must be reviewed for propriety by OCIO, Office of General Counsel (OGC), and/or the Freedom of Information Act (FOIA) office before being placed on Agency Web servers. Additionally, any material related to the operations of the aforementioned reviewing authorities must be reviewed and cleared in advance by the appropriate reviewing authority.

(4) Web servers must be operated and maintained by OCIO.

c. <u>Communications Servers</u> - Communication servers provide dial-in users access to the WAN. In addition to the foregoing, the following guidelines apply to communications servers:

(1) User accounts must be established for employees by the ASCPM upon presentation of an approved request signed by the appropriate program official. The employee will be given access to his/her LAN server and its associated privileges. No additional privileges will be granted.

(2) User accounts may not be shared. Users must not divulge their passwords to others.

(3) UNIX-level user accounts are not permitted on communication servers.

(4) Communications servers will be operated and maintained by OCIO.

d. <u>Internet Secure Servers</u> - Internet secure servers are established to permit secure communications between SBA, customers, and business partners via the Internet. In addition to the foregoing, the following guidelines apply to the secure servers:

(1) UNIX-level user accounts are not permitted on secure servers. The security agent of the server must generate Login IDs. Applications for user IDs must be approved by the ACSPM upon presentation of a request approved by the appropriate program office.

(2) Secure servers will be operated and maintained by OCIO. Program office requests for access to, or use of, secure servers, including necessary program development/modification, will be approved, coordinated, supervised, and accomplished by OCIO. Independent third party development of secure server applications is not permitted.

5. <u>What is the SBA Internet/Intranet Policy</u>?

In just 2 years, the Internet has become a major SBA resource. It has transformed the way SBA does business. SBA employees have access to a vast array of information on the Internet that enhances productivity and helps to serve clients more efficiently. Entrepreneurs and potential entrepreneurs now have access to SBA 24 hours a day via SBA's website (www.sba.gov). Because SBA's resource partners can now do business with SBA via the Internet, they can simplify and streamline their business processes.

While connection to the Internet offers many benefits, it also poses a significant risk to SBA data and system if you do not follow appropriate security guidelines or if you misuse services. Internet services are available to you to help you perform official SBA business, such as communicating with customers, researching relevant topics, and obtaining business information. The Internet use policy is designed to help you understand SBA's expectations for the use of Internet services and use the services wisely.

The following guidelines apply to use of SBA's Internet services:

(1) Already-existing SBA policies that apply to employee conduct in other circumstances may also apply to conduct on the Internet. This includes, but not limited to, policies on intellectual property protection, privacy, misuse of SBA assets or resources, sexual harassment, information and data security, and confidentiality.

(2) SBA software can monitor and record all Internet usage. So you should have no expectation of privacy in any Internet use, including e-mail messages that you create, send, or retrieve over the SBA Internet services. SBA may inspect any files stored in the SBA network and respond to reasonable requests from law enforcement and regulatory agencies for logs, diaries, and archives about employees' Internet use. If you use the Internet, you must identify yourself honestly, accurately, and completely, including your SBA affiliation and function, when requested.

(3) As with other SBA resources such as SBA's telephone and fax systems, you are allowed limited personal use of SBA's Internet services. You are authorized to make occasional personal use of the Internet, provided that such use is of short duration, does not adversely affect or hinder the mission of the SBA, and no fee is charged to SBA. Supervisors have management authority and responsibility to ensure that you appropriately use your official time and resources.

(4) If you do not follow this Internet policy, SBA may revoke your Internet privileges and/or take disciplinary action against you, including removal.

6. What Security Controls are Required for the SBA Wide Area Network (WAN)?

The WAN is the interconnection of SBA's Local Area Networks (LANs), Web and secure servers, and Internet connection. The WAN is divided into private and public networks. The private or "corporate" network contains the LANs, client servers, communication servers, and the mainframe system. The public network contains the Internet connection, web server(s), secure server(s), and bulletin board. The public network is separated from the private network by two firewalls.

The following guidelines apply to the WAN.

a. Corporate or sensitive data must not be placed on public systems. Corporate or sensitive data transmitted to approved destinations via the INTERNET or other public or semi-public networks must be encrypted via point-to-point session encryption. Acceptable encryption mechanisms include secure browsers (Netscape 4.0 or Microsoft Explorer 4.0, or above) to secure servers, secure telnet or ftp (source and destination), or other point-to-point encryption methods which can guarantee session decryption only by the intended recipient.

b. Public-side access to corporate data must be accomplished via SBA's secure servers. No other access method is permitted.

c. Dial-in access to the private network must be accomplished via communications servers. The use of directly connected modems must be phased-out as communications servers become available.

d. Connections to the private network from any source outside the network must be approved by OCIO before connection attempts are made. Once approved, all such connections must be secured with a filtering router and a dynamic filtering firewall system. The standard Agency firewall system is Checkpoint Technology's Firewall-1.

7. What Security Controls are Required for LANs?

The following guidelines must be implemented and followed on all SBA LANs (servers and workstations). The following guidelines are to be considered minimum requirements for operation of Agency LANs:

a. LAN Administrators must perform a daily full system backup on each server. Backups must be cycled through a minimum of 10 tapes (two-week cycle).

b. Accounts granted supervisory authority must be limited to the minimum required for administration of the LAN. Administrative passwords should be changed more frequently than the 90 days required for non-administrative users. Accounts must be reviewed monthly to determine continuing need.

c. With the exception of the System Administrator and his/her alternate, no employee will be granted permissions at the Root directory level (Global Permissions). Employees will be granted minimum access (normally 'read only' or 'read/execute') to needed directories. The general philosophy will be that users have no permissions unless specifically granted (as opposed to granting global permissions and then removing unneeded authority).

d. Users will be granted full access (read/write authority) to their personal data areas and the common shared area. Access to Application areas must be restricted to 'read only'. Access to System areas must be restricted to the LAN Administrator.

e. With the exception of the LAN Administrator, no accounts will be allowed concurrent access (multiple logins). Multiple logins defeat accountability.

f. Accounts must not be created for a specific application/function unless absolutely necessary. If created, permissions must be granted only for that application or function and station restricted.

g. All LAN users must be assigned unique accounts.

h. All accounts must be password protected. Passwords must be a minimum of eight characters. Passwords must automatically expire every 90 days. 'Grace' logins must be limited to three.

i. ‘Guest' accounts must be deactivated. Personnel requiring temporary access to a LAN must be issued a temporary user-id with an expiration date commensurate with need.

j. Accounts must be deleted immediately when an employee leaves an organization. LAN accounts must be monitored monthly for excess accounts.

k. Users must not store non-share data in the common shared area. Common areas are reserved for temporary storage of working group files (files that need to be accessed by other employees). Non-shared data must be stored in the employee's home directory on the LAN.

l. All system and application files, where possible, must be flagged as 'read only'.

m. OCIO must approve connections to the private network from any source outside the network before connection attempts are made.

8. What are the Security Policies on the Use of Electronic Mail (E-mail) Service Provided by SBA?

The following policies apply to all SBA employees, contractor personnel, and vendors using E-mail service provided by SBA:

a. E-mail facilities operated by or for SBA are for official use only and are subject to the same restrictions on their use and to the same review process as any other Government furnished resource provided for the use of employees.

b. Messages and files contained within SBA E-mail systems are considered Agency property and are subject to examination in connection with authorized official Agency reviews (e.g. OIG investigations, audits and inspections, administrative inquiries and reviews, etc.).

E-mail messages and files may be classified as official or Agency records with mandatory retention periods. The Agency records officer will establish Agency policy on E-mail file and record retention.

E-mail messages are considered official SBA documents, which means that they are subject to administrative review under the FOIA and the Privacy Act (PA). E-mail messages should, therefore, be drafted with appropriate discretion. If printed or stored E-mail messages are deemed responsive to a request for information made pursuant to either Act, those items must be reviewed for disclosure in accordance with the provisions of the FOIA and/or the PA.

c. Information about individuals in electronic form (including E-mail) should be protected to the same extent as a written record and be disclosed only when required for authorized purposes. In addition, commercial proprietary information should be protected in accordance with the conditions under which it is provided.

d. Unauthorized reading, disclosure, modification, or deletion of E-mail messages addressed to others is strictly prohibited. Violations of this provision will be addressed within established Agency policies and guidelines on employee conduct.

e. Individuals with E-mail accounts on Agency LANs must use all security measures available to secure their E-mail messages from review by unauthorized personnel. At a minimum, all password facilities must be enabled on Agency E-mail accounts.

f. Individuals needing additional information concerning the use of E-mail for particular actions (e.g. FOIA requests, filing of grievances, etc.) should consult the SOP that covers the specific action.

NOTE: Employees may not use E-mail to file FOIA and PA requests, or Agency or union grievances. SBA does accept E-mail FOIA requests from the public.

g. The CIO is responsible for developing, coordinating, and disseminating Agency E-mail policy and ensuring that Agency units have implemented appropriate procedures. Managers are responsible for ensuring that their employees are informed of the above policy.

9. <u>What are the Security Control Requirements for Development of a Sensitive Automated Application?</u>

a. Security requirements and specifications must be defined by the ACSPM in conjunction with the responsible program office. The application security plan must take into account the security of all systems in which the application will operate. These requirements must be incorporated into the overall systems design requirements.

b. Assign security responsibilities for each major application to a member of management who is knowledgeable in the nature of the information and the process supported by the application and in the management, personnel, operational, and technical controls used to protect it. This person shall be contacted when a security incident occurs concerning the designated application.

c. Management controls must be in place to ensure that sensitive applications are not approved for programming development until security specifications are included in the system specifications.

d. A sensitive automated application must require formal certification prior to the application being placed into operation.

e. Test procedures must be implemented to verify the adequacy of the programmed security controls prior to being placed into operation.

10. What is the Continuity of Operations Program?

a. The Continuity of Operations program is a contingency plan developed to ensure continued operations in the event of a disaster or extended loss of processing power.

b. An AIS contingency plan must be in force to facilitate the timely recovery of data processing operations in the event of a disaster or extended loss of processing power.

c. The implementation of appropriate contingency plans must be the responsibility of the system manager, installation director, or regional administrator. Guidance, coordination, and assistance must be available from the ACSPM and the OCIO Disaster Recovery Manager.

d. A contingency plan must be prepared and tested annually for each major application, each regional and district computing activity, the Office of Financial Operations, and the SBA's main computer center. Each contingency plan must address three areas:

(1) Emergency procedures,

(2) Backup operations, and

(3) Recovery procedures.

e. The contingency planning process will consider:

(1) Extent of emergencies,

(2) Essential applications,

(3) Backup alternatives,

(4) Backup resources,

(5) Contingency plan tests, and

(6) Contingency plan maintenance.

f. Tests of the contingency plan must be documented and retained for one year. Test documentation should include but not be limited to:

(1) Personnel participating in the contingency test,

(2) Reflect the application(s) tested,

(3) Include initial planning meeting minutes,

(4) Provide high-level test criteria, and

(5) Reflect test results including obstacles and resolution, action items, exception conditions and resolution.

11. What are the Policies for Personnel Security?

a. ADP positions within SBA that involve programming, operation, design, or use of automated information systems or data must be evaluated as "critical sensitive," “non-critical," or "non-sensitive" using guidelines established by the Office of Personnel Management (5 CFR Parts 731 and 732), the OIG (SOP 90 21), and the Office of Human Resources (SOP to be issued at a later date).

b. Contractor personnel occupying ADP positions designated as critical-sensitive must not access SBA sensitive data until an appropriate clearance has been granted.

c. A Position Sensitivity Level Determination Form must be completed by the ACSPM for each contractor position on SBA contracts for ADP services. A copy of the form must be forwarded to the Director, Office of Security Operations, OIG.

d. All SBA and contractor employees who have access to sensitive data must be made fully aware of their responsibilities for protecting sensitive data and for detecting and preventing misuse of AIS resources.

12. What are the Security Policies for SBA ADP Contracts?

SBA contracts that require contractors to access the SBA Computer System must include the requirements below:

a. General.

The contractor must establish administrative, technical, and physical security measures at its computer facility to protect sensitive SBA information from unauthorized disclosure or misuse and to prevent unauthorized access to the contractor’s computer system. The contractor must describe in the proposal the specific measures that will be taken to meet this requirement. SBA reserves the right to inspect the contractor's security measures, data handling procedures, and other security safeguards to determine the security posture of the contractor facility.

b. Protection of Sensitive SBA Data.

Physical access to the contractor's office areas that contain sensitive SBA data must be controlled to prevent unauthorized personnel from acquiring access to this data.

Contractors who are authorized to access the SBA Network Security System must ensure that telephone numbers of the SBA Computer System, log-on passwords, identifiers, and access procedures, are safeguarded from unauthorized use and disclosure. Contractor personnel must comply as follows:

(1) Read and sign the Computer Access/Clearance Form.

(2) Change passwords quarterly.

(3) Promptly notify the Contracting Officer's Technical Representative (COTR) when a contractor personnel is no longer authorized access to the SBA Computer System.

(4) The contractor must not release SBA data outside of its facility, either orally or in written form, without the express written consent of SBA. All requests received by the contractor for SBA data must be referred to SBA for action.

(5) When the contract specifies the handling of sensitive data, the contractor must agree to permit an inspection by authorized SBA personnel during the performance of the contract to ensure the continued efficacy and efficiency of safeguards and the discovery and countering of new threats and hazards. Authorized SBA personnel include the ACSPM, the COTR, the OIG, and other personnel designated by the CIO.

c. Contractor Background Investigations.

(1) As a condition for access to Government-owned systems and data, contractor personnel must pass background investigations in accordance with OMB Circular A-130, which requires screening of all individuals involved with sensitive applications or data in Federal automated information systems. All SBA automated systems and data are considered sensitive.

(2) A SBA official or its designated representative will perform background investigations.

(3) The ACSPM will assign each contract labor category a security sensitivity rating which will determine the type of background investigation performed for the labor category position(s).

(4) The Director, Office of Security and the ACSPM will review investigation results. The COTR will notify the contractor of the results of the investigation.

(5) The COTR must immediately notify the ACSPM when contract personnel are hired, identifying the contractor's name, labor category, and date of entry on duty. The ACSPM will provide appropriate forms and instructions to the COTR for transmission to the contract personnel. Completed forms must be returned directly to the ACSPM within two weeks from date of issuance.

APPENDIX 3

ABBREVIATIONS

1.	ACSPM	Agency Computer Security Program Manager
2.	ADP	Automated Data Processing
3.	AIS	Automated Information System
4.	CIO	Chief Information Officer
5.	DIRM	District Information Resource Manager
6.	DSO	District Security Officer
7.	ESC	Eagan Service Center – Unisys Corporation
8.	FITS	Field Information Technology Specialist
9.	HQ	Headquarters
10.	GAO	General Accounting Office
11.	ISO	Installation Security Officer
12.	OIG	Office of Inspector General
13.	OCIO	Office of the Chief Information Officer
14.	D/DSO	District/Disaster Security Officer
15.	SBA	Small Business Administration